



8e6® ProxyBlocker

QUICK START GUIDE



Model: ProxyBlocker
MSA-004-005

Release: 1.0.00 / Updated: 02.11.08

8E6 PROXYBLOCKER QUICK START GUIDE

© 2008 8e6 Technologies. All rights reserved.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# PBA-MSAul-QSG-080211

CONTENTS

8E6 PROXYBLOCKER INTRODUCTION	1
About this Document	2
Conventions Used in this Document.....	2
SERVICE INFORMATION	3
PRELIMINARY SETUP PROCEDURES	4
Unpack the Unit from the Carton	4
Select a Site for the Server	5
Rack Mount the Server.....	6
Check the Power Supply.....	15
General Safety Information.....	16
INSTALL THE SERVER	19
Step 1: Setup Procedures.....	19
Step 1A: Wizard Setup Procedures	20
Step 1B: Console Setup Procedures.....	27
Step 2: Test the ProxyBlocker Console Connection.....	37
Step 3: Test Filtering	38
Step 4: Set Library Updates.....	38
CONCLUSION	41
LED INDICATORS AND BUTTONS.....	42
MSA Units.....	42
REGULATORY SPECIFICATIONS AND DISCLAIMERS.....	43
Declaration of the Manufacturer or Importer	43
INDEX	45

8E6 PROXYBLOCKER INTRODUCTION

Thank you for choosing to evaluate the 8e6 Technologies ProxyBlocker. The ProxyBlocker offers a solution for organizations using an Internet filtering product other than 8e6's R3000 Enterprise Filter. 8e6 ProxyBlocker tracks each user's online activity of Web-based proxies and anonymizers, and can be configured to block specific Web sites or service ports, thereby protecting your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources.

About this Document

This document is divided into the following sections:

- **Introduction** - This section is comprised of an overview of the ProxyBlocker product and how to use this document
- **Service Information** - This section provides 8e6 Technologies contact information
- **Preliminary Setup Procedures** - This section includes instructions on how to physically set up the ProxyBlocker in your network environment
- **Install the Server** - This section explains how to configure the ProxyBlocker for filtering
- **Conclusion** - This section indicates that the quick start steps have been completed
- **LED Indicators and Buttons** - This section explains how to read LED indicators and use LED buttons for troubleshooting the unit
- **Regulatory Specifications and Disclaimers** - This section cites safety and emissions compliance information for the ProxyBlocker model referenced in this document
- **Index** - An alphabetized list of some topics included in this document

Conventions Used in this Document

The following icons are used throughout this document to call attention to important information pertaining to handling, operation, and maintenance of the server; safety and preservation of the equipment, and personal safety:



NOTE: *The “note” icon is followed by additional information to be considered.*



WARNING: *The “warning” icon is followed by information alerting you to a potential situation that may cause damage to property or equipment.*



CAUTION: *The “caution” icon is followed by information warning you that a situation has the potential to cause bodily harm or death.*

SERVICE INFORMATION

The user should not attempt any maintenance or service on the unit beyond the procedures outlined in this document.

Any initial hardware setup problem that cannot be resolved at your internal organization should be referred to an 8e6 Technologies solutions engineer or technical support representative.

8e6 Corporate Headquarters (USA)

Local : 714.282.6111
Domestic US : 1.888.786.7999
International : +1.714.282.6111

8e6 Taiwan

Taipei Local : 2397-0300
Domestic Taiwan : 02-2397-0300
International : 886-2-2397-0300

Procedures

When calling 8e6 Technologies regarding a problem, please provide the representative the following information:

- Your contact information.
- Serial number or original order number.
- Description of the problem.
- Network environment in which the unit is used.
- State of the unit before the problem occurred.
- Frequency and repeatability of the problem.
- Can the product continue to operate with this problem?
- Can you identify anything that may have caused the problem?

PRELIMINARY SETUP PROCEDURES

Unpack the Unit from the Carton

Inspect the packaging container for evidence of mishandling during transit. If the packaging container is damaged, photograph it for reference.

Carefully unpack the unit from the carton and verify that all accessories are included. Save all packing materials in the event that the unit needs to be returned to 8e6 Technologies.

The carton should contain the following items:

- 1 ProxyBlocker unit
- 1 AC Power Cord
- 1 Serial Port Cable
- 1 CAT-5E Crossover Cable
- Rack Mount Brackets (2)
- 1 End User License Agreement (EULA)
- 1 envelope containing a CD-ROM with PDFs of the ProxyBlocker User Guide and ProxyBlocker Authentication User Guide. The latest version of the ProxyBlocker User Guide can be obtained from our Web site at http://www.8e6.com/docs/pba_ug.pdf. The latest version of the ProxyBlocker Authentication User Guide can be obtained from our Web site at http://www.8e6.com/docs/pba_auth_ug.pdf.



NOTES: A coupler is included in the carton if a three-foot CAT-5E crossover cable was packaged with your unit instead of a 14-foot CAT-5E crossover cable.

Inspect the server and accessories for damage. If the contents appear damaged, file a damage claim with the carrier immediately.



WARNING: To avoid danger of suffocation, do not leave plastic bags used for packaging the server or any of its components in places where children or infants may play with them.

Select a Site for the Server

The server operates reliably within normal office environmental limits. Select a site that meets the following criteria:

- Clean and relatively free of excess dust.
- Well-ventilated and away from sources of heat, with the ventilating openings on the server kept free of obstructions.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields and noise caused by electrical devices such as elevators, copy machines, air conditioners, large fans, large electric motors, radio and TV transmitters, and high-frequency security devices.
- Access space provided so the server power cord can be unplugged from the power supply or the wall outlet—this is the only way to remove the AC power cord from the server.
- Clearance provided for cooling and airflow: Approximately 30 inches (76.2 cm) in the back and 25 inches (63.5 cm) in the front.
- Located near a properly earthed, grounded, power outlet.


Rack Mount the Server

Rack Setup Precautions

 **Warning:**


Before rack mounting the server, the physical environment should be set up to safely accommodate the server. Be sure that:


- The weight of all units in the rack is evenly distributed. Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- The rack will not tip over when the server is mounted, even when the unit is fully extended from the rack.
- For a single rack installation, stabilizers are attached to the rack.
- For multiple rack installations, racks are coupled together.
- Reliable earthing of rack-mounted equipment is maintained at all times. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- A power cord will be long enough to fit into the server when properly mounted in the rack and will be able to supply power to the unit.
- The connection of the server to the power supply will not overload any circuits. Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- The server is only connected to a properly rated supply circuit. Reliable earthing (grounding) of rack-mounted equipment should be maintained.
- The air flow through the server's fan or vents is not restricted. Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- The maximum operating ambient temperature does not exceed 104°F (40°C). If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.

 **WARNING:** *Extend only one component at a time. Extending two or more components simultaneously may cause the rack to become unstable.*

Rack Mount Instructions

Optional: Install the Chassis Rails


 **NOTE:** If your chassis does not come with chassis rails, please follow the procedure listed on the last page of this sub-section to install the unit directly into the rack.

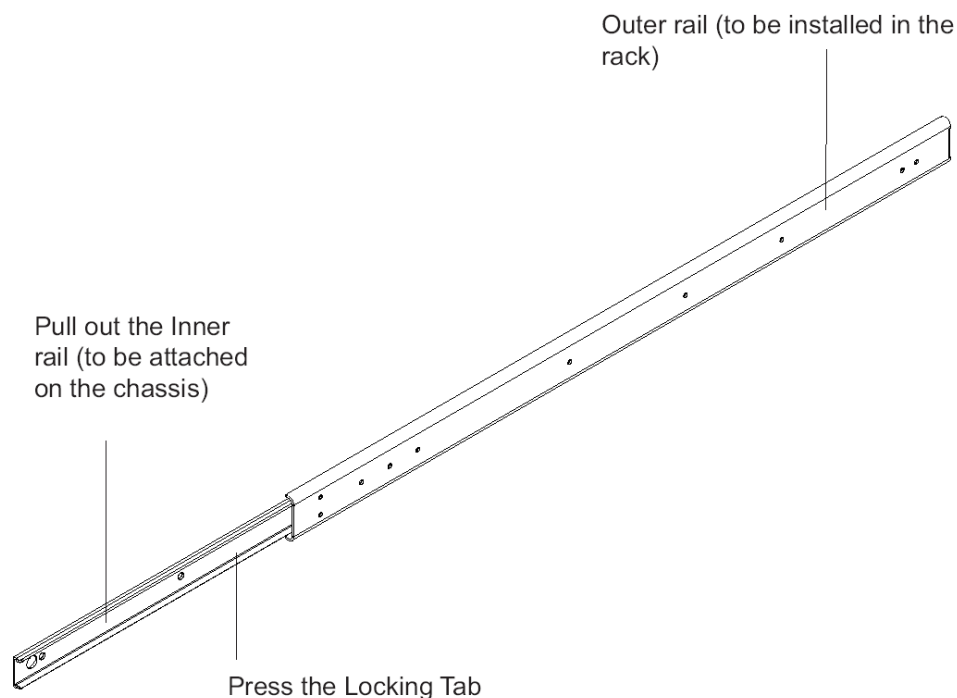
 **CAUTION:** Please make sure that the chassis covers and chassis rails are installed on the chassis before you install the chassis into the rack. To avoid personal injury and property damage, please carefully follow all the safety steps listed below:

Before installing the chassis rails:

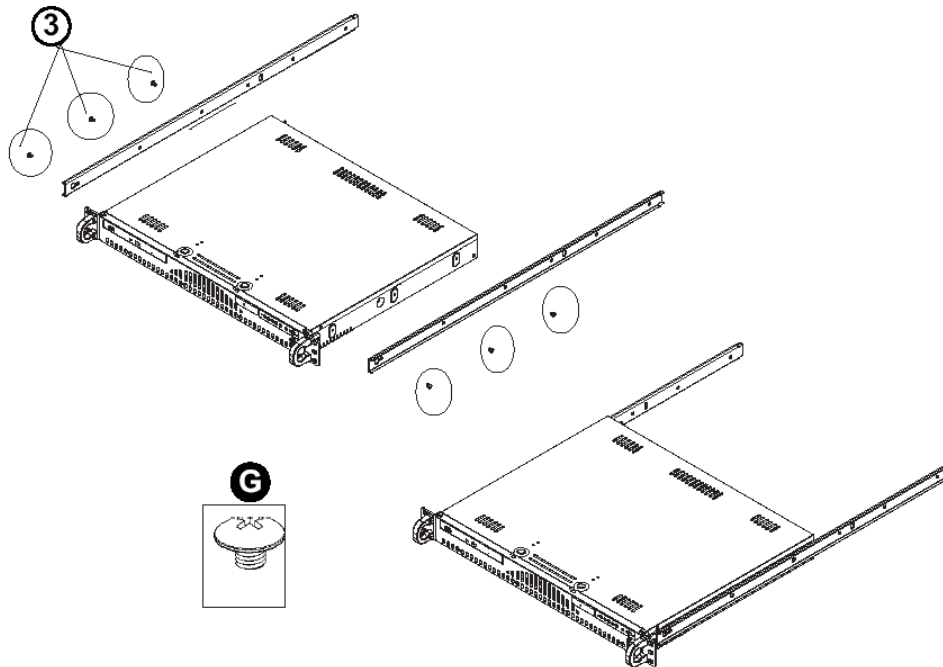
- Close the chassis using the chassis cover.
- Unplug the AC power cord(s).
- Remove all external devices and connectors.

1. Included in the shipping package are a pair of rail assemblies. In each rail assembly, locate the inner rail and the outer rail.
2. Press the locking tab to release the inner rail from its locking position and pull out the inner rail from the rail assembly.

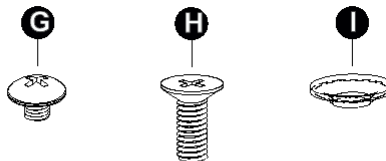
 **NOTE:** The inner rails are to be attached to the chassis and the outer rails are to be installed in the rack.



3. Locate the three holes on each side of the chassis and locate the three corresponding holes on each of the inner rail.



4. Attach an inner rail to each side of the chassis and secure the inner rail to the chassis by inserting three Type G screws through the holes on each side of the chassis and the inner rail. (See the diagram below for a description of the Type G screw.)



- G. Round head M4 x 4 mm [0.157]
- H. Flat head M5 x 12 mm [0.472]
- I. Washer for M5

5. Repeat the above steps to install the other rail on the chassis.

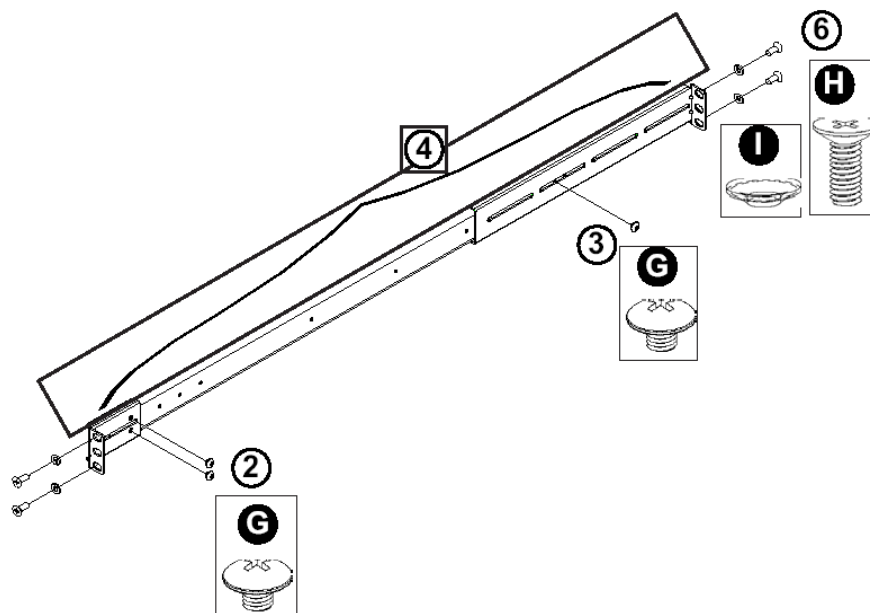
Optional: Install the Traditional UP Racks

After you have installed the inner rails on the chassis, you are ready to install the outer rails of rail assemblies to the rack.


 **NOTE:** The rails are designed to fit in the racks with the depth of 28" to 33".

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest server components on the bottom of the rack first, and then work up.

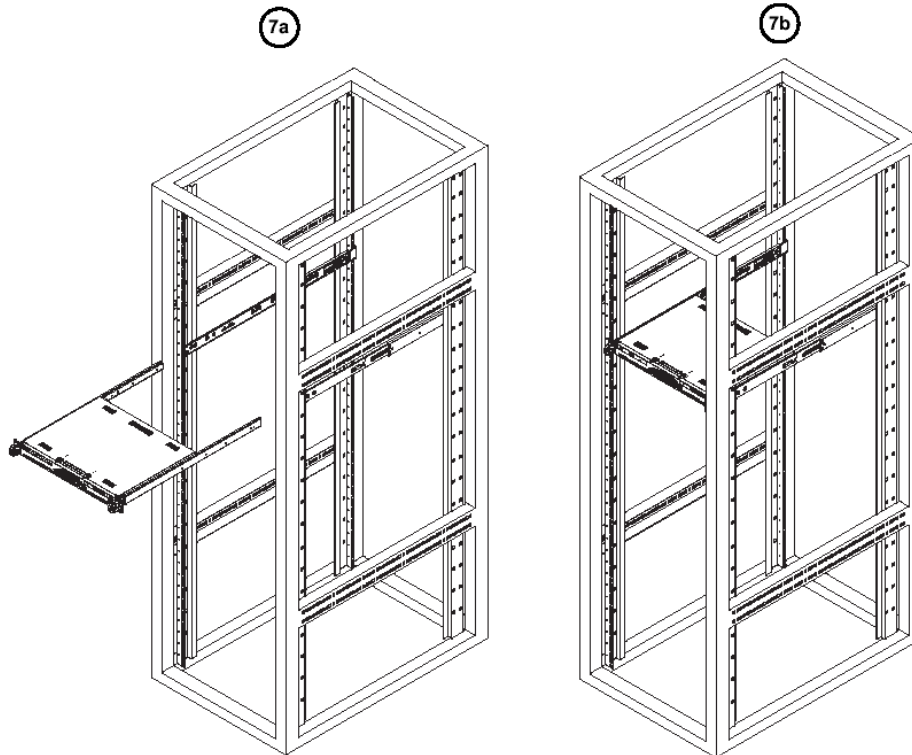
1. In the package, locate a pair of front (short) and rear (long) brackets. Please note that the brackets are marked with Up/Front Arrows (front) and Up/Rear arrows (rear).
2. Secure the front (short) bracket (marked with the Up/Front arrows) to the outer rail with two Type G screws. (See the previous page for a description of the Type G screw.)
3. Attach the rear (long) bracket to the other end of the outer rail and secure the rear (long) bracket to the outer rail with a Type G screw as shown below.
4. Measure the depth of your rack and adjust the length of the rails accordingly.
5. Repeat the same steps to install the other outer rail on the chassis.
6. Secure both outer rail assemblies to the rack with Type H screws and Type I washers. (See the previous page for descriptions of Type H and Type I hardware components.)



- Slide the chassis into the rack as shown below.

 **NOTE:** The chassis may not slide into the rack smoothly or easily when installed the first time. Some adjustment to the slide assemblies might be needed for easy installation.

- You will need to release the safety taps on both sides of the chassis in order to completely remove the chassis out of the rack.

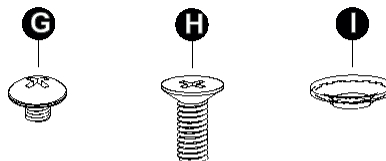
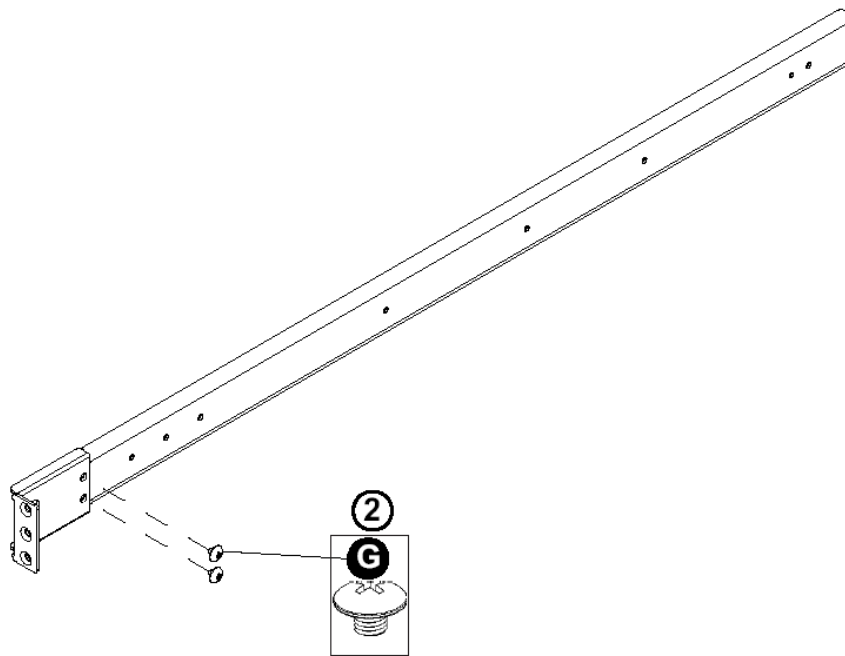


Optional: Install the Open Racks

After you have installed the inner rails on the chassis, you are ready to install the outer rails of rail assemblies to the rack.

 **NOTE:** The rails are designed to fit in the racks with the depth of 28" to 33".

- Determine the placement of each component in the rack before you install the rails.
 - Install the heaviest server components on the bottom of the rack first, and then work up.
1. In the package, locate a pair of front (short) and rear (long) brackets. Please note that the brackets are marked with Up/Front Arrows (front) and Up/Rear arrows (rear).
 2. Secure the front (short) bracket (marked with the Up/Front arrows) to the outer rail with two Type G screws as shown below.

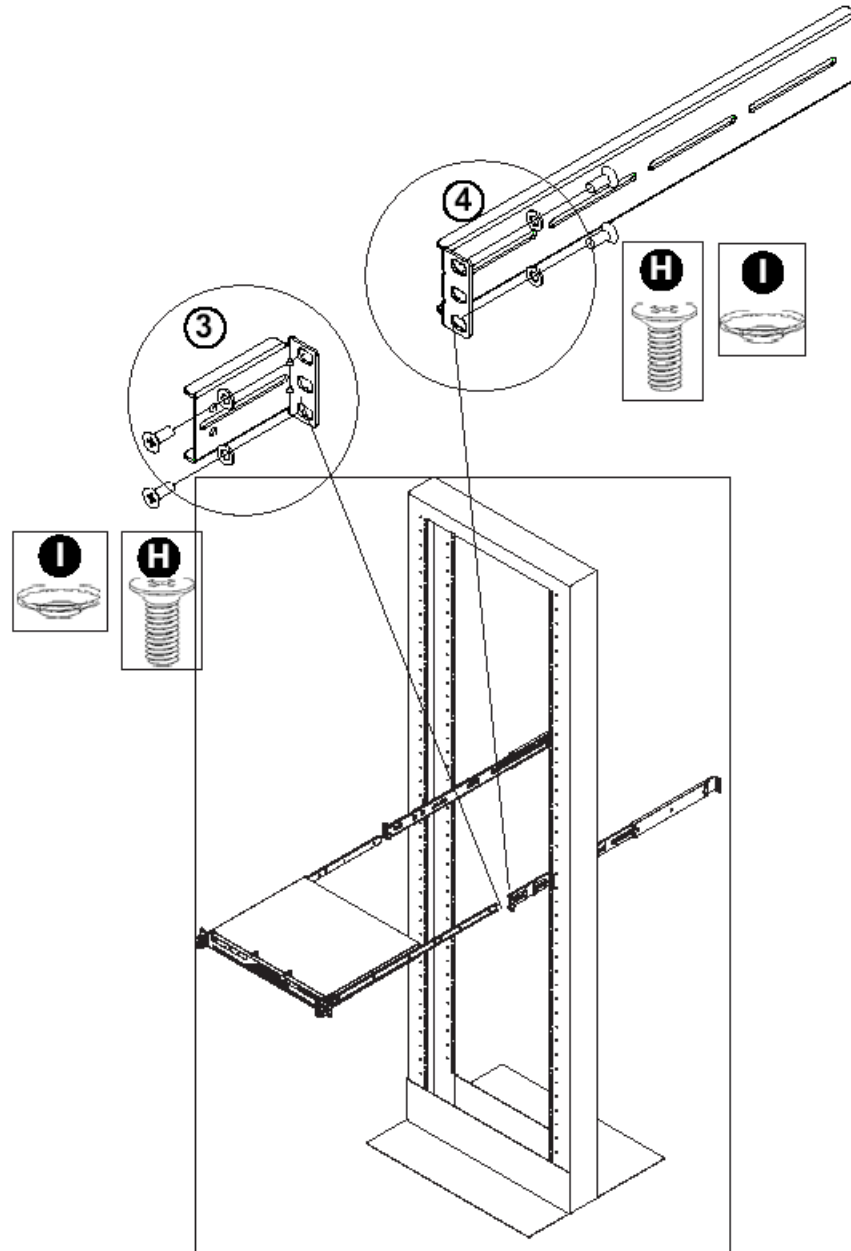


G. Round head M4 x 4 mm [0.157]

H. Flat head M5 x 12 mm [0.472]

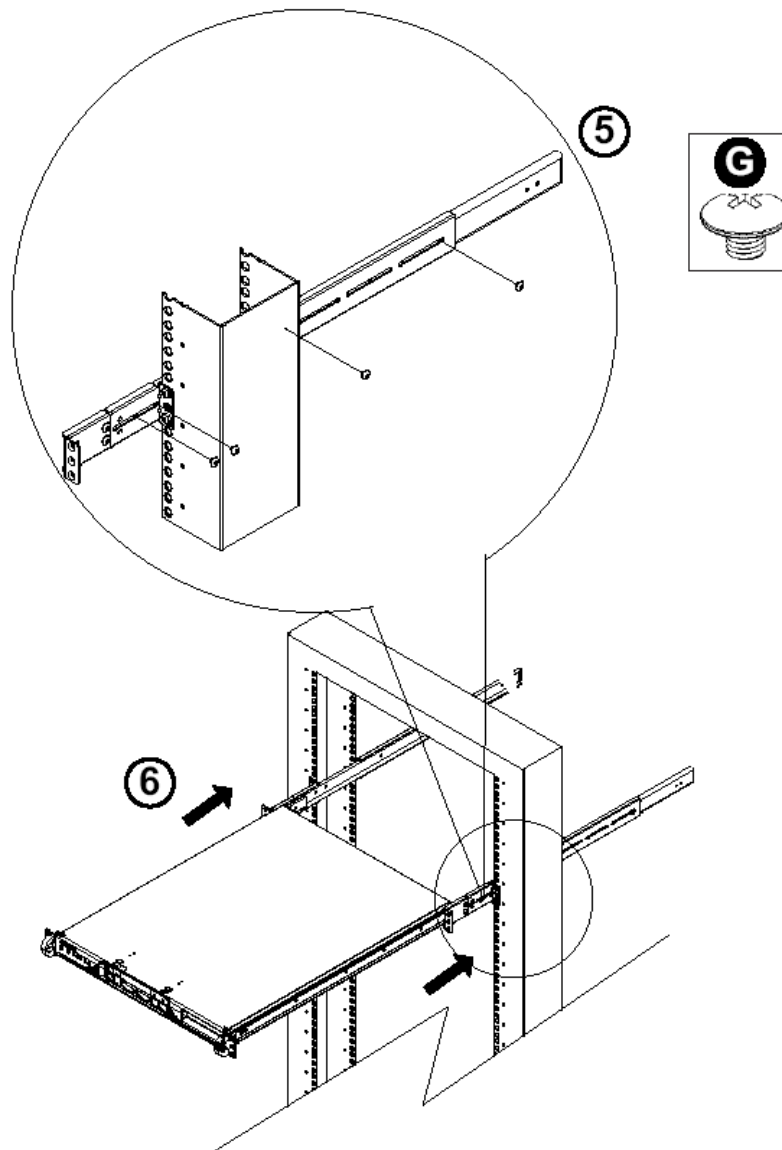
I. Washer for M5

3. Attach the front (short) bracket to the front end of the rack, and secure it to the rack with two Type H screws and Type I washers as shown below. (See the previous page for descriptions of Type H and Type I hardware components.)
4. Attach the rear (long) bracket to the rear end of the rack, and secure it to the rack with two Type H screws and Type I washers as shown below. Repeat the same steps to install the other outer rail to the other side of rack.



5. Measure the depth of your rack and adjust the length of the rails accordingly. Then, secure the rails to the chassis with Type G screws.

- Slide the inner rails which are attached to the chassis into the outer rails on the rack.

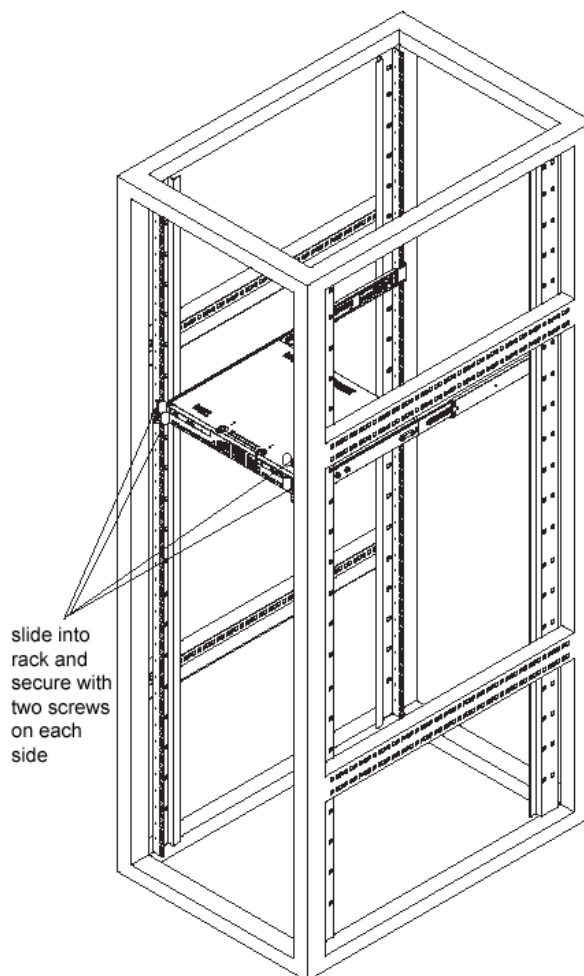


Install the Chassis into the Rack

 **CAUTION:** Before installing the chassis into the rack:

- Make sure that the rack is securely anchored onto an unmovable surface or structure before installing the chassis into the rack.
- Unplug power cord(s) of the rack before installing the chassis into the rack.
- Make sure that the system is adequately supported. Make sure that all the components are securely fastened to the chassis to prevent components falling off from the chassis.
- The rack assembly should be properly grounded to avoid electric shock.
- The rack assembly must provide sufficient airflow to the chassis for proper cooling.
- Please make sure that all components and all chassis covers are properly installed in the chassis before you install the chassis into the racks; otherwise, out-of-warranty damage may occur.

Slide the chassis into the rack and secure it with two screws on each side of the rack as shown in the picture.



Check the Power Supply

This server is equipped with a universal power supply that handles 100-240 V, 50/60 Hz. A standard power cord interface (IEC 950) facilitates power plugs that are suitable for most European, North American, and Pacific Rim countries.

Power Supply Precautions

 **Warning:**


- Use a regulating uninterruptible power supply (UPS) to protect the server from power surges, voltage spikes and to keep the server operating in case of a power failure.
- In geographic regions that are susceptible to electrical storms, 8e6 highly recommends plugging the AC power cord for the server into a surge suppressor.
- Use appropriately rated extension cords or power strips only.
- Allow power supply units to cool before touching them.


General Safety Information


Server Operation and Maintenance Precautions


 **Warning:**

Observe the following safety precautions during server operation and maintenance:

 **WARNING:** *If the server is used in a manner not specified by the manufacturer, the protection provided by the server may be impaired.*

 **WARNING:** *8e6 Technologies is not responsible for regulatory compliance of any server that has been modified. Altering the server's enclosure in any way other than the installation operations specified in this document may invalidate the server's safety certifications.*

 **CAUTION:** *Never pile books, papers, or other objects on the chassis, drop it, or subject it to pressure in any other way. The internal circuits can be damaged, and the battery may be crushed or punctured. Besides irreparable damage to the unit, the result could be dangerous heat and even fire.*

 **CAUTION:** *There are no user-serviceable components inside the chassis. The chassis should only be opened by qualified service personnel. Never disassemble, tamper with, or attempt to repair the server. Doing so may cause smoke, fire, electrical shock, serious physical injury, or death.*

- Do not insert objects through openings in the chassis. Doing so could result in a short circuit that might cause a fire or an electrical shock.
- Do not operate the server in an explosive atmosphere, in the presence of flammable gases.
- To ensure proper cooling, always operate the server with its covers in place. Do not block any openings on the chassis. Do not place the server near a heater.
- Always exit the software application properly before turning off the server to ensure data integrity.
- Do not expose the server to rain or use near water. If liquids of any kind should leak into the chassis, power down the server, unplug it, and contact 8e6 Technologies technical support.
- Disconnect power from the server before cleaning the unit. Do not use liquid or aerosol cleaners.

AC Power Cord and Cable Precautions


Warning:

- The AC power cord for the server must be plugged into a grounded, power outlet.
- Do not modify or use a supplied AC power cord if it is not the exact type required in the region where the server will be installed and used. Replace the cord with the correct type.
- Route the AC power cord and cables away from moving parts and foot traffic.
- Do not allow anything to rest on the AC power cord and cables.
- Never use the server if the AC power cord has been damaged.
- Always unplug the AC power cord before removing the unit for servicing.

Electrical Safety Precautions

Warning:

Heed the following safety precautions to protect yourself from harm and the server from damage:

 **CAUTION:** *Dangerous voltages associated with the 100-240 V AC power supply are present inside the unit. To avoid injury or electrical shock, do not touch exposed connections or components while the power is on.*

- To prevent damage to the server, read the information in this document for selection of the proper input voltage.
- Do not wear rings or wristwatches when troubleshooting electrical circuits.
- To avoid fire hazard, use only the specified fuse(s) with the correct type number, voltage, and current ratings. Only qualified service personnel should replace fuses.
- Qualified service personnel should be properly grounded when servicing the unit.
- Qualified service personnel should perform a safety check after any service is performed.

Motherboard Battery Precautions

 **Caution:**

The battery on the motherboard should not be replaced without following instructions provided by the manufacturer. Only qualified service personnel should replace batteries.

The battery contains energy and, as with all batteries, a malfunction can cause heat, smoke, or fire, release toxic materials, or cause burns. Do not disassemble, puncture, drop, crush, bend, deform, submerge or modify the battery. Do not incinerate or expose to heat above 140°F (60°C).

There is a danger of explosion if the battery on the motherboard is installed upside down, which will reverse its polarities.

CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISPOSE OF THE USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

ATTENTION: IL Y A DANGER D'EXPLOSION S'IL Y A REMPLACEMENT INCORRECT DE LA BATTERIE, REMPLACER UNIQUEMENT AVEC UNE BATTERIE DU MÊME TYPE OU D'UN TYPE ÉQUIVALENT RECOMMANDÉ PAR LE CONSTRUCTEUR. METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÈMENT AUX INSTRUCTIONS DU FABRICANT.

INSTALL THE SERVER

Step 1: Setup Procedures

This step requires you to link the workstation to the ProxyBlocker. You have the option of using the text-based wizard setup procedures described in Step 1A, or the Administrator console setup procedures described in Step 1B.

Wizard Setup Requirements

The following hardware can be used for the wizard setup procedures:

- ProxyBlocker with AC power cord
- either one of two options:
 - PC monitor with AC power cord and keyboard, or
 - PC laptop computer with HyperTerminal and serial port cable (and USB DB9 serial adapter, if there is no serial port on your laptop)

Go to Step 1A to execute Wizard Setup Procedures.

Administrator Console Setup Requirements

The following hardware is required for the Administrator console setup procedures:

- ProxyBlocker unit with AC power cord
- CAT-5E crossover cable
- PC laptop computer, or PC monitor with AC power cord and keyboard

Go to Step 1B to execute Console Setup Procedures.

Step 1A: Wizard Setup Procedures

Link the Workstation to the ProxyBlocker

Monitor and Keyboard Setup

- A. Connect the PC monitor and keyboard cables to the rear of the chassis:



Fig. 1 - Portion of chassis rear

- B. Turn on the PC monitor.
- C. Power on the ProxyBlocker by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 2).

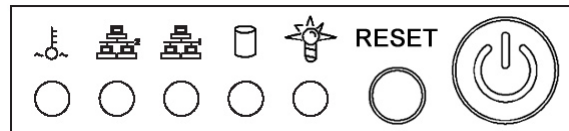


Fig. 2 - Diagram of chassis front panel, power button at far right

Once the ProxyBlocker is powered up, proceed to the Login Screen instructions.

Serial Console Setup

- A. Using the serial port cable (and USB DB9 serial adapter, if necessary), connect the laptop to the rear of the chassis (see Fig. 1).
- B. Power on the laptop.
- C. Power on the ProxyBlocker by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 2).

Once the ProxyBlocker is powered up, proceed to the instructions for HyperTerminal Setup Procedures.

HyperTerminal Setup Procedures

If using a serial console, follow these procedures to create a HyperTerminal session on the serial console.

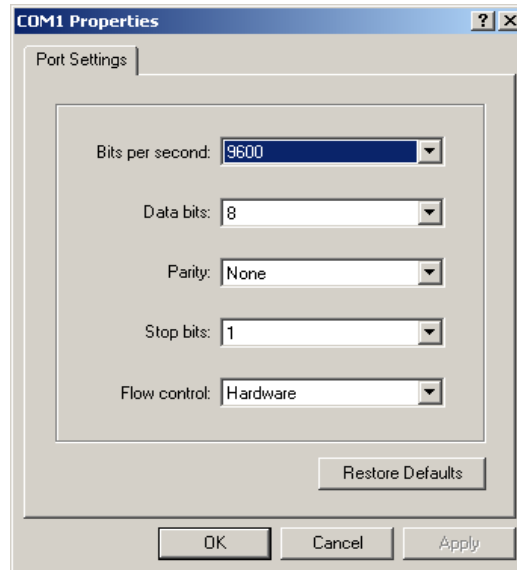
- A. Launch HyperTerminal by going to Start > Programs > Accessories > Communications > HyperTerminal:



- B. In the Connection Description dialog box, enter any session **Name**, and then click **OK** to open the Connect To dialog box:



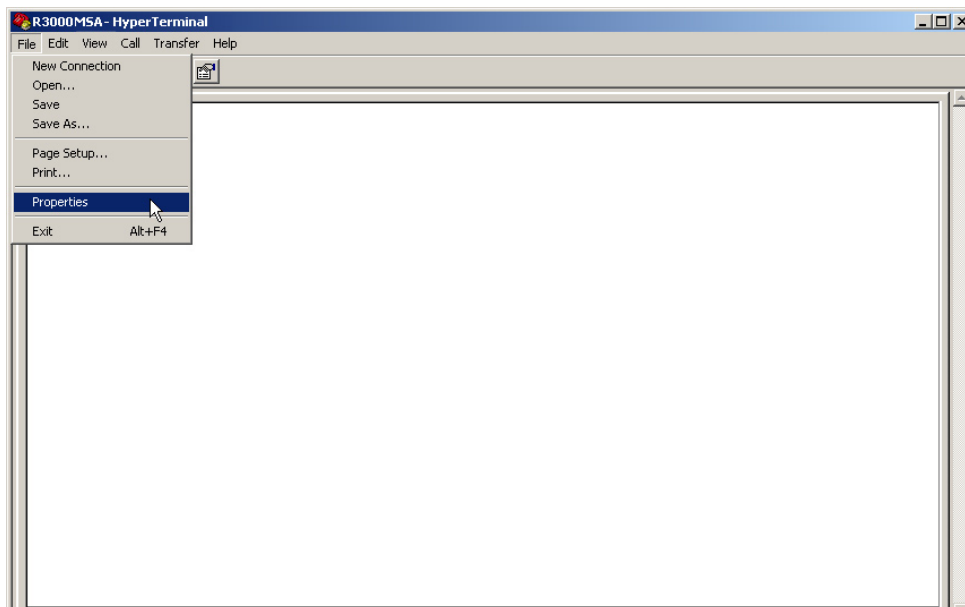
- C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably “COM1”), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:



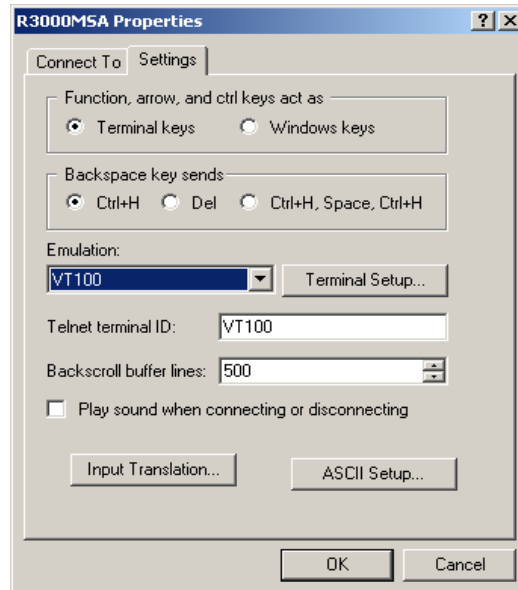
- D. Specify the following session settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware


- E. Click **OK** to connect to the HyperTerminal session:



- F. In the HyperTerminal session window, go to File > Properties to open the Properties dialog box, displaying the Connect To and Settings tabs:




- G. Click the Settings tab, and at the **Emulation** menu select "VT100".
- H. Click **OK** to close the dialog box, and to go to the login screen.

 **NOTE:** If using a HyperTerminal session, the login screen will display with black text on a white background.

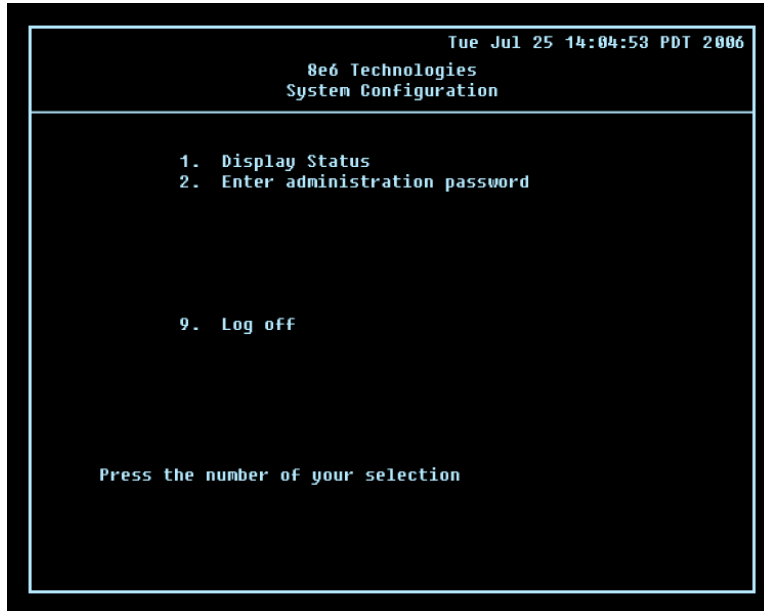
Login screen

The login screen displays after powering on the ProxyBlocker unit.

 **NOTE:** If the screensaver currently displays on your screen, press the **Enter** key to display the login screen.

- A. At the **login** prompt, type in **menu**.
- B. Press the **Enter** key to display the Password prompt.
- C. At the **Password** prompt, type in the following: **#s3tup#r3k**
- D. Press **Enter** to display the System Configuration screen.

System Configuration Screen



- A. At the **Press the number of your selection** prompt, press **2** to select the setup process for the System Configuration wizard.
- B. At the login prompt, re-enter your password: **#s3tup#r3k**
- C. Press **Enter** to display the Administration menu where you can begin using the System Configuration wizard.

System Configuration: Administration menu

```

Tue Jul 25 14:05:16 PDT 2006
8e6 Technologies
System Configuration - Administration menu

1. Display Status
2. Initial Setup wizard
3. Configure network interface LAN1
4. Configure network interface LAN2
5. Configure default gateway
6. Configure DNS servers
7. Configure host name
8. Time Zone regional setting
A. Reset system to factory defaults
B. Reboot system
C. Change administrator password

X. Exit administration menu

Press the number of your selection

```

- A. At the **Press the number of your selection** prompt, press **2** to select the “Initial Setup wizard” process.

The wizard takes you to the following system configuration screens to make entries:

- Configure network interface LAN1
- Configure network interface LAN2
- Configure default gateway
- Configure DNS servers
- Configure host name
- Time Zone regional setting



NOTE: See the Network screens for LAN Settings and Regional Setting in Step 1B for content included in the wizard screens.

- B. After making all entries using the wizard, press **X** to return to the System Configuration screen. Or, to verify the status of the ProxyBlocker and review the entries you made using the wizard, press **1** to view the System Status screen.



NOTES: Changing your password using option C, “Change administration password”, will change the password for the console menu but not the ProxyBlocker console login screen. Option A, “Reset system to factory defaults”, should only be used by an 8e6 Technologies technical representative.

System Status Screen

```

Tue Jul 25 14:05:16 PDT 2006
8e6 Technologies
System Status - updates every 10 seconds

LAN1 is the Capturing Interface
LAN1 IP = 1.2.3.4 Mask = 255.255.255.255      Inactive
LAN2 is the Management and Blocking Interface
LAN2 IP = 200.10.160.74 Mask = 255.255.0.0   Active
Default gateway IP: 200.10.160.1
ProxyBlocker host name: logo.com

DNS server IP address(es): 200.10.160.1
Regional timezone setting: US/Pacific

ProxyBlocker processing is initializing
Current Version: ProxyBlocker 1.0.00.8
Library was last updated on 2007/06/15

Press any key to return to menu...

```

The System Status screen contains the following information:

- **Capturing Interface** specified in screen 3 (Configure network interface LAN1)
- **LAN1 IP** address and netmask specified in screen 3, and current status (“Active” or “Inactive”)
- **Management and Blocking Interface** specified in screen 4 (Configure network interface LAN2)
- **LAN2 IP** address and netmask specified in screen 4, and current status (“Active” or “Inactive”)
- **Default gateway** IP address specified in screen 5 (Configure default gateway)
- **ProxyBlocker host name** specified in screen 7 (Configure host name)
- **DNS server IP address(es)** specified in screen 6 (Configure DNS servers)
- **Regional timezone setting** specified in screen 8 (Time Zone regional setting)
- Current status of the ProxyBlocker
- Current ProxyBlocker software **Version** installed
- Library update status



NOTE: Modifications can be made at any time by returning to the specific screen of the wizard.

Log Off, Disconnect the Peripherals

- After completing the wizard setup procedures, return to the System Configuration screen and press **9** to log out.
- Disconnect the peripherals from the ProxyBlocker.

Step 1B: Console Setup Procedures

Preliminary Setup

Create a “setup workstation” using a Windows-based laptop or desktop machine with a network card and Internet Explorer 5.5 (or later). The setup workstation will be used for accessing the ProxyBlocker server on the network and configuring the unit.



NOTE: *The Java Plug-in version specified for the ProxyBlocker software version must be installed on your workstation. If your workstation does not have Java Runtime Environment, you will be prompted to install it.*

Workstation Configurations

- A. From the desktop of the setup workstation, follow the procedures for your machine type:
 - **Windows XP** - go to Start > Control Panel. Open Network Connections. Right-click the link for LAN or High-Speed Internet and choose Properties.
 - **Windows 2000** - right-click the My Network Places icon and select Properties. Right-click the correct Local Area Connection and choose Properties.
 - **Windows NT** - right-click the Network Neighborhood icon and select Properties.
 - **Windows ME** - right-click the My Network Places icon and select Properties.
- B. Click on **Internet Protocol (TCP/IP)** to highlight it (Windows NT and ME users should select the Protocols or Configuration tab and choose **TCP/IP Protocol**).
- C. Click the **Properties** button.




WARNING: *Be sure to make note of the current network settings on the setup workstation as you will need to return them for further setup procedures.*

- D. Choose the option **Use the following IP address** (Windows NT and ME users should choose the option **Specify an IP Address**).
- E. Type in the **IP address** of 1.2.3.1.
- F. Type in the **Subnet mask** (netmask) of 255.0.0.0 and click **OK**.
- G. Close the LAN connection properties box.

Link the Workstation to the ProxyBlocker

The procedures outlined in this sub-section require the use of the CAT-5E crossover cable.


- A. Plug one end of the CAT-5E crossover cable into the ProxyBlocker's **LAN 2** port.

 **NOTE:** When facing the rear of the chassis, the LAN 2 port is the port on the right.




Portion of chassis rear

- B. Plug the other end of the CAT-5E crossover cable into the setup workstation's network card.

 **NOTE:** If a CAT-5E coupler was packaged with your unit, this coupler can be used if the crossover cable is not long enough for your setup. Plug one end of the CAT-5E crossover cable into the ProxyBlocker, and the other end into the coupler. Plug a standard CAT-5E cable into the other end of the coupler, and the free end of the standard CAT-5E cable into the setup workstation.

- C. Plug the ProxyBlocker into a power source with an appropriate rating.

 **WARNING:** It is strongly suggested you use an uninterruptible power supply.

- D. Power on the ProxyBlocker by lowering the bezel and pressing the large button at the right of the front panel (see diagram below):

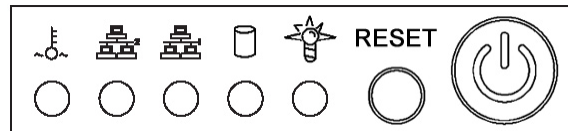


Diagram of chassis front panel, power button at far right

The Boot Up Process

The boot-up process may take 5 - 10 minutes. When the drive light remains off for 30 seconds, the system is booted up. (See the LED Indicators and Buttons section for a description of Front LED Indicators and Buttons for Hardware Status Monitoring.)

If you wish to verify that the unit has been booted up, you can perform the following test on your workstation:

1. Go to your taskbar and click Start > Run.
2. In the dialog box, type in **cmd** (type in **command** if using Windows ME).
3. Click **OK**.
4. In the cmd.exe window, type in **ping 1.2.3.4**
5. Press **Enter** on your keyboard.

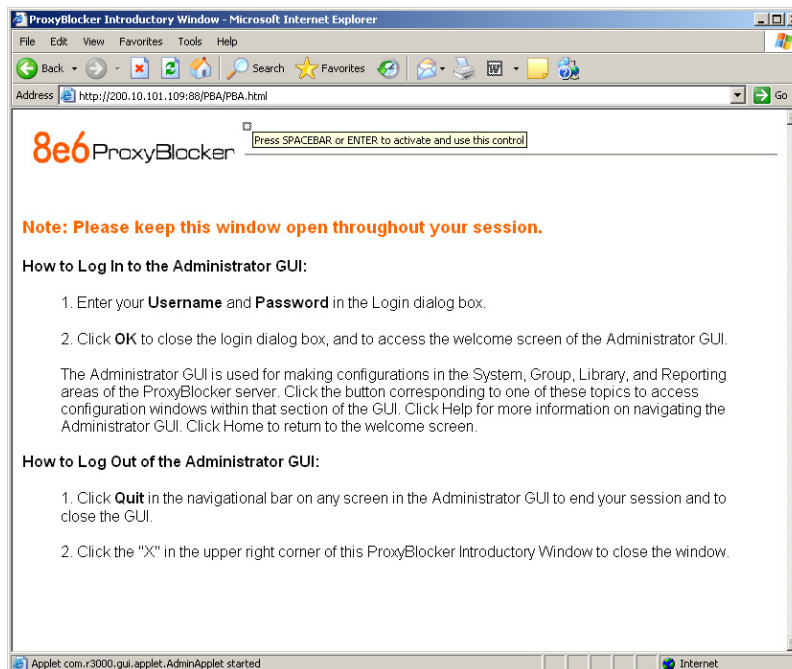
If you receive a reply, the unit is up.

Network Setup

When the ProxyBlocker is fully booted, you can configure network settings. For this step, you will need your network administrator to provide you the host name, gateway address, and two unused IP addresses.

Access the ProxyBlocker Administrator Console

- A. Launch Internet Explorer from the setup workstation.
- B. Type in **http://1.2.3.4:88** in the address field.
- C. Click **Go** to open the ProxyBlocker Introductory Window:

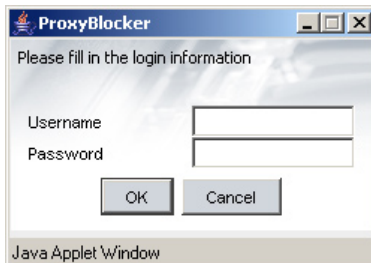


NOTE: This window must be left open throughout your session.

The Introductory Window displays minimized when the login dialog box of the Proxy-Blocker Administrator console application opens (see image on the next page).

Log in to ProxyBlocker Administrator Console

In the login dialog box, you need to enter the generic Username and Password:



A Java Applet Window titled "ProxyBlocker" with a standard Windows-style title bar. The window contains the text "Please fill in the login information". Below this text are two input fields: "Username" and "Password". At the bottom of the window are two buttons: "OK" and "Cancel". The status bar at the bottom of the window reads "Java Applet Window".

- A. In the **Username** field, type in **admin**.
- B. In the **Password** field, type in **user3**.
- C. Click **OK** to close the login dialog box and to go to the main screen of the Proxy-Blocker Administrator console:



The main screen of the ProxyBlocker Administrator console. The window title is "ProxyBlocker". The header area features the "8e6 ProxyBlocker" logo and a navigation menu with buttons for "HOME", "SYSTEM", "GROUP", "LIBRARY", "REPORTING", "HELP", and "QUIT". The main content area is divided into two sections. On the left is a "Welcome" message: "Welcome to the ProxyBlocker management console. This screen displays product and system status information. Click the System, Group, Library, or Reporting tab to access corresponding configuration properties. Click Help for information on navigating the management console. To return to this screen, click the Home button. Click Quit to exit the console." On the right is the "8e6 Technologies" logo and the text "8e6 ProxyBlocker User Interface". Below this is a table showing system status information:

Product	
ProxyBlocker Version Number	ProxyBlocker 1.0.00.4
ProxyBlocker Status	
Last Patch Update	05/18/2007
Last Library Update	06/03/2007

At the bottom of the window, there is a status bar with the following information: "Host Name: logo.com", "IP: 200.10.100.75", and "Version: ProxyBlocker 1.0.00.4". The status bar also indicates "Java Applet Window".


Network

Click the **System** button at the top of the screen to go to the System section of the console:



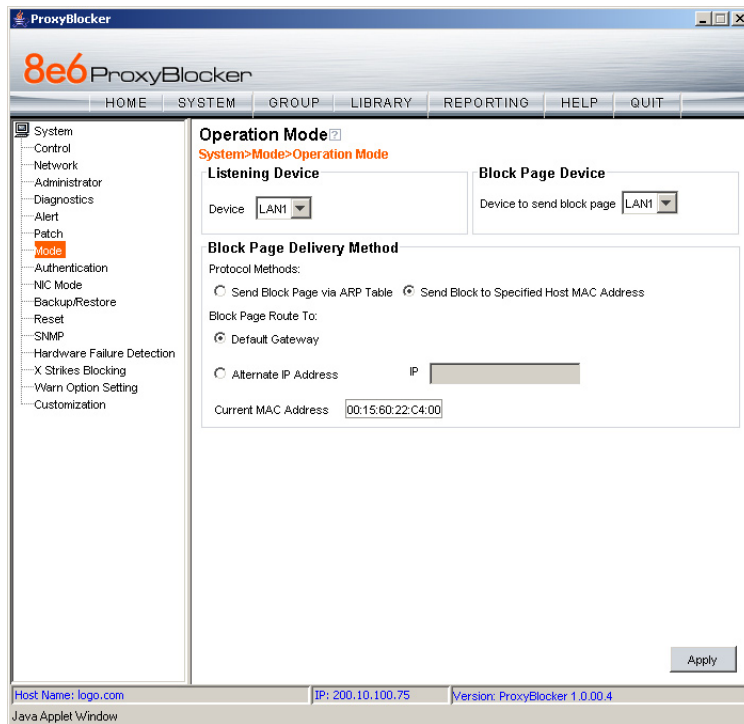
In this section of the console you will:

- Specify the device(s) the ProxyBlocker will use for listening to traffic and sending traffic
- Configure LAN settings the ProxyBlocker will use on your network
- Select NTP servers the ProxyBlocker will use for time synchronization with Internet clocks
- Indicate the region in which the ProxyBlocker is geographically located

 **NOTE:** After saving your entries in each of these windows (Operation Mode, LAN Settings, NTP Servers, Regional Setting), you may be prompted to restart or reboot the server. Click **OK** to acknowledge the contents of the alert box, and then proceed to the next sub-step **without** restarting or rebooting the server.

Network: Operation Mode

From the navigation panel at the left of the screen, click Mode and choose Operation Mode from the pop-up menu:

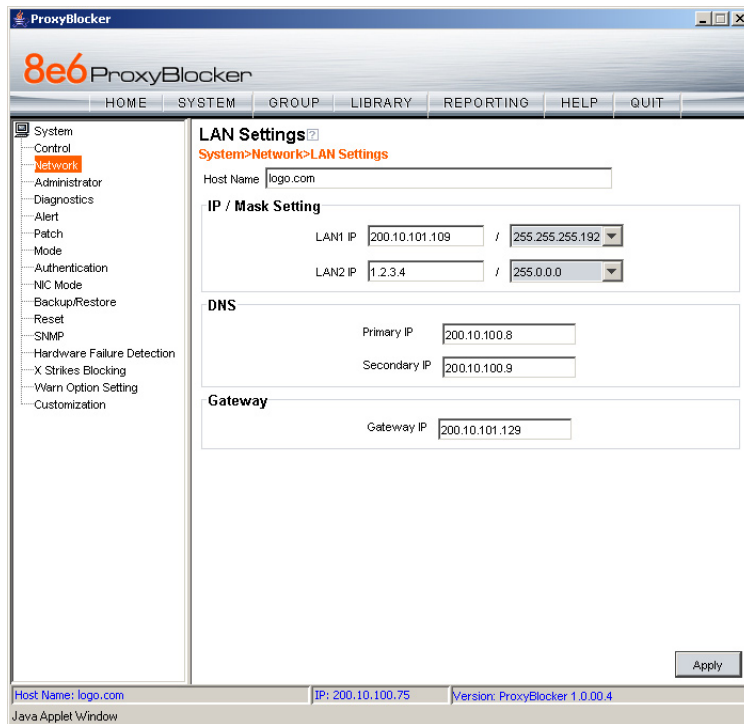


Make the following entries in the Operation Mode window:

- A. In the Listening Device frame, select the device for listening to traffic, generally “LAN1”.
- B. In the Block Page Device frame, select the device for sending block pages to client PCs. The block page device should be a different device than the one selected in the Listening Device frame—“LAN2” is generally used as the default device for sending block pages
- C. Click **Apply**.

Network: LAN Settings

From the navigation panel, click Network and choose LAN Settings from the pop-up menu:



Make the following entries for the ProxyBlocker in the LAN Settings window:

- A. Enter the **Host Name** that includes your domain name, for example PBASERVER.myserver.com (the NetBIOS name must be capitalized). It is important to enter something identifiable, because once the product is registered, this host name is used by 8e6 Technologies to recognize your account for library updates. This name needs to be a valid DNS entry.
- B. Enter the **LAN1 IP** address and specify the subnet for LAN 1, the ProxyBlocker's first Ethernet Network Interface Card (NIC).

You may use a non-routeable IP address for the listening interface and a subnet mask of 255.255.255.255 (32 bites).

- C. Enter the **LAN2 IP** address and subnet for LAN 2, the ProxyBlocker's second Ethernet NIC. The subnet selection is usually 255.255.0.0 (16 bites) or 255.255.255.0 (24 bites), **but cannot be 255.255.255.255 (32 bites)**.
- D. Enter the **Primary IP** address of the first DNS name server. The ProxyBlocker uses this name server to resolve the domain name requested by users from the LAN.

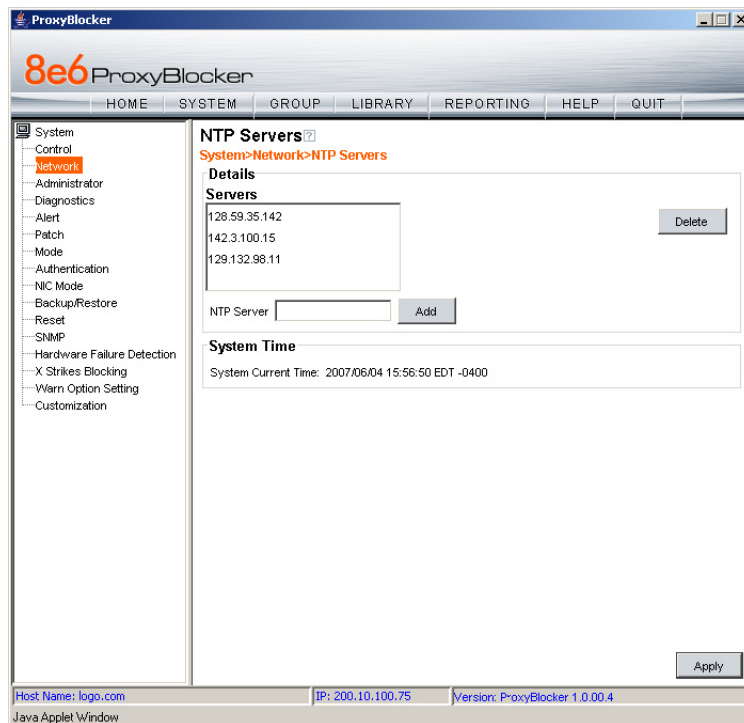
- E. Enter the **Secondary IP** address of the second DNS name server. The ProxyBlocker will use this name server to resolve the domain name requested by users from the LAN if the first DNS isn't working.
- F. Enter the **Gateway IP** address for the default router or firewall that is the main gateway for the entire network. The ProxyBlocker will use this IP address to communicate outside the network.

⚠ WARNING: Be sure to take note of the LAN 1 and LAN 2 IP addresses and host name you assigned to the ProxyBlocker. It is strongly suggested you document and store this information as it is now the only way of communicating with the ProxyBlocker.

- G. Click **Apply**.


Network: NTP Servers

From the navigation panel, click Network and choose NTP Servers from the pop-up menu:




The NTP Servers window is used for specifying the Network Time Protocol (NTP) servers to be used by the ProxyBlocker, so that the ProxyBlocker is synchronized with computer clocks on the Internet.

Note that the following server IP addresses display in the Servers list box: 128.59.35.142, 142.3.100.15, 129.132.98.11. If necessary, any of these servers can be deleted by selecting the IP address and clicking **Delete**.

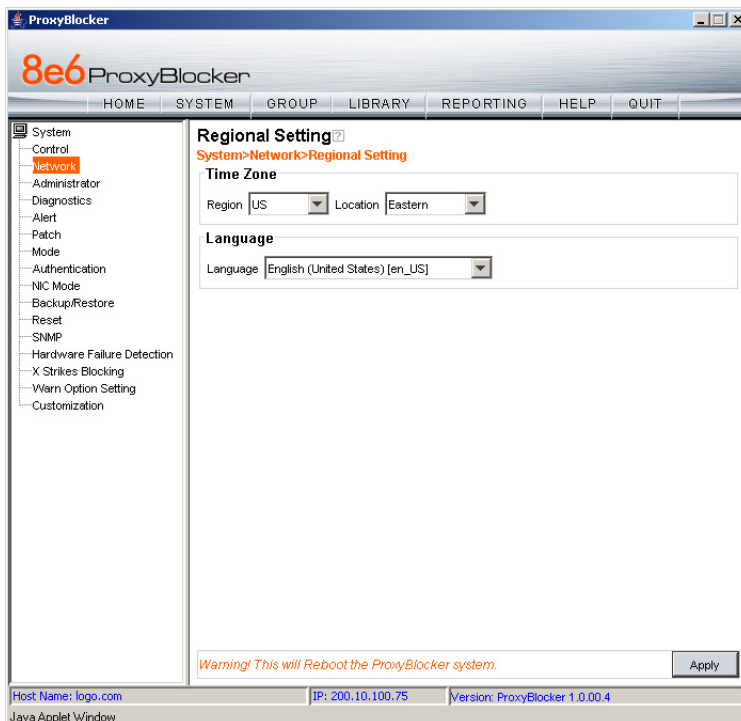
 **NOTE:** If you need to find another NTP server to use, most university Web sites provide these servers for public usage.

- A. In the **NTP Server** field, enter the IP address of the primary NTP server you wish to use for clock settings on your server.
- B. Click **Add** to include this IP address in the Servers list box.
- C. Enter two more NTP servers, following the procedures in sub-steps A and B. These will be the secondary and tertiary NTP servers, in order as they appear in the list box.
- D. Click **Apply**.

 **NOTE:** If the primary server fails, the secondary will be used. If the secondary server fails, the tertiary server will be used.

Network: Regional Setting

From the navigation panel, click Network and choose Regional Setting from the pop-up menu:



Make the following selections in the Regional Setting window:

- A. At the **Region** pull-down menu, select your country from the available choices.

- B. At the **Location** pull-down menu, select the time zone for the specified region.

If necessary, select a language set from the **Language** pull-down menu to display that text in the console.

- C. Click **Apply** to apply your settings, and to reboot the ProxyBlocker.

Physically Connect the ProxyBlocker to the Network

Once your ProxyBlocker network parameters are set, you must physically connect the unit to your network. This step requires two standard CAT-5E cables.



NOTE: *This section requires you to restart the ProxyBlocker. If you wish to relocate the ProxyBlocker before connecting it to the network, you must first shut down the server instead of restarting it. To shut down the ProxyBlocker, go to the navigation panel, click Control, and then select ShutDown. Once the server is shut down, you must power on the ProxyBlocker and then log back into the Administrator console.*

- A. Restart the server using the steps defined below (i-iii). These steps must always be performed when restarting the ProxyBlocker. **Never** reset the server by using the power or reset buttons.
- i. From the navigation panel of the System section of the console, click Control and select Reboot from the pop-up menu to display the Reboot window.
 - ii. Click the **Reboot** button.
 - iii. From the time you click Reboot, you have approximately 2 minutes to perform sub-steps B through E while the ProxyBlocker goes through the reboot process.
- B. Disconnect the crossover cable from the ProxyBlocker.
- C. Plug one end of a standard CAT-5E cable into the ProxyBlocker's LAN 1 port.
- D. Plug the other end of the CAT-5E cable into an open port on the network hub that handles the Internet traffic you wish to filter.
- E. Repeat sub-steps B and C for the ProxyBlocker's LAN 2 port.
- F. Wait until the reboot process has completed, indicated by the drive light staying off for 30 seconds. This process may take 5 to 10 minutes. Proceed to Step 2.



NOTES: *If you receive a connection failure message during the reboot process, please disregard it, as this often occurs when there is a change in the IP address.*

To restart the browser window, close both the ProxyBlocker Administrator console and the ProxyBlocker Introductory Window. Begin a new session by opening a new browser window and then logging back into the Administrator console.

Step 2: Test the ProxyBlocker Console Connection

Now that the ProxyBlocker is physically installed on your network and you have configured its network settings, you need to test the unit to see if it is set up properly.

- A. Restore the setup workstation you used for the Network Setup to its original settings, and connect it to the network hub to create a “network workstation.” (You could also use another workstation already on the network that has Internet access.)
- B. Launch IE on the network workstation, and enter the IP address you assigned to LAN 1 (Step 1A, System Configuration: Administration menu, or Step 1B, Network: LAN Settings, sub-step B). Be sure to include the port information :88 in the address field. For example, if the ProxyBlocker were assigned an IP address of 10.10.10.10, you would enter **http://10.10.10.10:88** in the browser window’s address field.
- C. Click **Go**. You should be prompted to log into the Administrator console, giving the Username and Password.

If you can access the ProxyBlocker Administrator console, the ProxyBlocker is functioning on your network and you should proceed to Step 3.

If you cannot access the ProxyBlocker Administrator console, please verify the status of the LAN connection in Windows on the network workstation, and then try enabling/disabling the LAN connection. If that fails to work, check the following:

- The ProxyBlocker is turned on.
- The ProxyBlocker is connected to the same hub as your router/firewall.
- Can the PC normally connect to the Internet?
- Is the PC able to ping LAN 1 of the ProxyBlocker?
- Is the ProxyBlocker plugged into a switch instead of a hub?
- Is there a caching server?
- Can the ProxyBlocker ping the filtered PC? (Refer to the System Command window in the Diagnostics section of the ProxyBlocker User Guide)
- Did you restart the ProxyBlocker after changing the network settings?
- Do you have both LAN ports connected to your network hub?
- If still unsuccessful, contact an 8e6 Technologies solutions engineer or technical support representative.

Step 3: Test Filtering

Once you have accessed the ProxyBlocker Administrator console, you should test filtering.

- A. Test the ProxyBlocker's filtering by opening a browser window on a network workstation, and going to **http://test.8e6.net** (an empty site for testing pornography filtering).
- B. You should receive a block page. If you do not, contact an 8e6 Technologies solutions engineer or technical support representative.



NOTE: Port 22 (SSH) must be open on your network to allow access by remote technical support.

Step 4: Set Library Updates

After verifying that the ProxyBlocker is correctly installed on your network, you need to activate ProxyBlocker library updates. Library updates are critical for filtering as new sites are added to the 8e6 library each day. To activate updates, visit the 8e6 Technologies Web site and enter the activation code that was issued to you by e-mail (also included on the product invoice).



NOTE: Ports 20 and 21 (FTP) must be open for outgoing requests so that the ProxyBlocker can receive library updates.

Activate and Register the ProxyBlocker

Be sure you have a valid host name chosen before activating your account.

- A. Open an Internet browser window and go to **http://www.8e6.com/activate**.
- B. After reading through the online End User License Agreement, click **Accept** to go to Step 2 of the activation process.
- C. Enter your activation code.
- D. Click **Submit** to go to the ProxyBlocker Activation and Registration page.
- E. Verify that your serial number and activation code are the same as shown on this registration page.
- F. Fill out the information on this page, including the host name for the public DNS server. **The entry of the unique host name you've chosen is mandatory in order to receive library updates.**
- G. After all information is entered, click **Activate** to activate your service. You should receive confirmation that the ProxyBlocker at your host name has been activated.

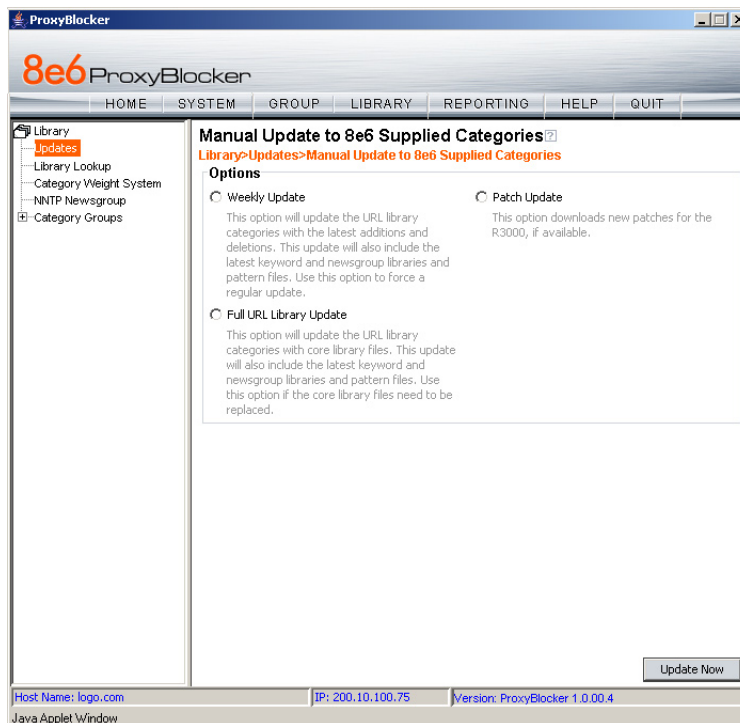
You may wish to print the confirmation page for future reference in dealing with technical issues.

Perform a Complete Library Update

Your ProxyBlocker was shipped with the latest library update for the current software release. However, as new updates continually become available, before you begin using the ProxyBlocker you must perform a complete library update to ensure you have the latest library updates.

To download the latest library updates, go to the ProxyBlocker Administrator console.

- A. Click the **Library** button at the top of the screen.
- B. From the navigation panel, click Updates and select Manual Update from the menu:

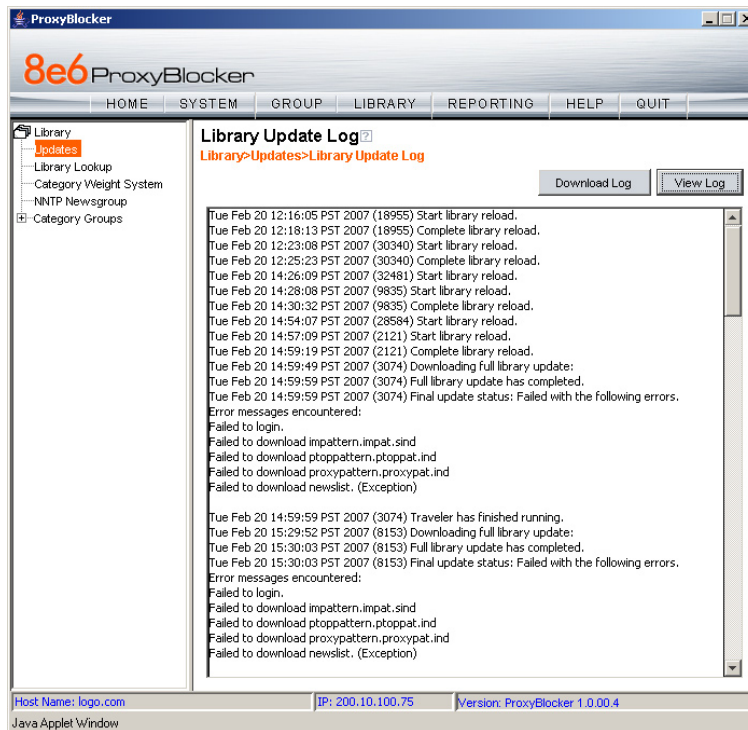



- C. In the Manual Update to 8e6 Supplied Categories window, click the radio button corresponding to **Full URL Library Update**.
- D. Click **Update Now** to begin the update process.


Monitor the Library Update Process

To verify that the library is being updated:

- A. From the navigation panel, click Updates and select Library Update Log from the menu.
- B. In the Library Update Log window, click **View Log** to display the update activity:



 **NOTE:** You will be notified in the log when the library has been completely updated by the message: "Full URL Library Update has completed." If this message does not yet display, click **View Log** again to view the latest information.

 **WARNING:** At the conclusion of this step, your ProxyBlocker will be actively filtering your network. The ProxyBlocker is initially set to filter pornography sites on all of your network traffic associated with the hub to which it is connected.

CONCLUSION

Congratulations; you have completed the ProxyBlocker quick start procedures. Now that the ProxyBlocker is filtering your network, the next step is to set up groups and create filtering profiles for group members.

To activate a default filter profile more appropriate for your operations, or to specify a more limited IP range to filter, consult Chapter 2: Group screen in the Global Administrator Section of the ProxyBlocker User Guide. Refer to Chapter 1: System screen for information on how to give end users access to acceptable HTTPS sites if strict HTTPS filtering settings are used.

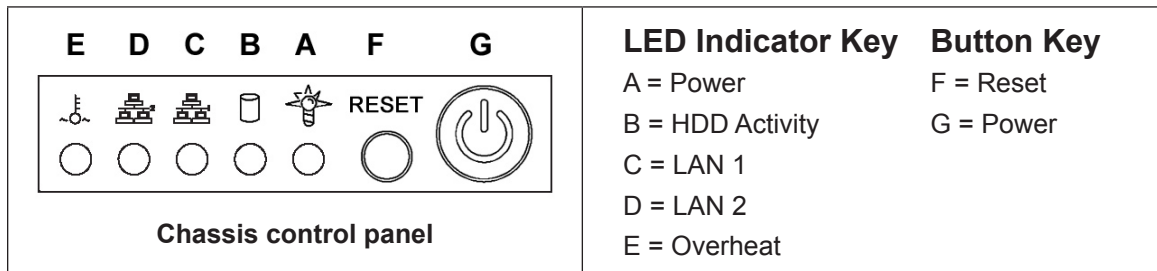
Obtain the latest ProxyBlocker User Guide at http://www.8e6.com/docs/pba_ug.pdf.

LED INDICATORS AND BUTTONS

MSA Units

Front LED Indicators and Buttons for Hardware Status Monitoring

LED indicators and buttons for hardware status monitoring display on the front panel, located on the right side of the chassis (see diagram below).



LED indicators alert you to the status of a feature on the unit while buttons let you perform a function on the unit.

LED Indicator	Color	Condition	Description
Power	Green	On	System On
		Off	System Off
HDD	Amber	Blinking	HDD Activity
		Off	No HDD Activity
LAN 1 & LAN 2	Green	On	Link Connected
		Blinking	LAN Activity
		Off	Disconnected
Overheat	Red	On	System Overheated
		Off	System Normal

REGULATORY SPECIFICATIONS AND DISCLAIMERS

Declaration of the Manufacturer or Importer

Safety Compliance

USA:	UL 60950-1 2nd ed. 2007
Europe:	Low Voltage Directive (LVD) 2006/95/EC to CB Scheme EN 60950: 2006
International:	UL/CB to IEC 60950-1:2006

Electromagnetic Compatibility (EMC)

USA:	FCC CFR 47 Part 15, Verified Class A Limit
Canada:	IC ICES-003 Class A Limit
Europe:	EMC Directive, 2004/108/EC & Low Voltage Directive (LVD) 2006/95/EC

Federal Communications Commission (FCC) Class A Notice (USA)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Declaration of Conformity

Model: MSA-004-005

Electromagnetic Compatibility Class A Notice

Industry Canada Equipment Standard for Digital Equipment (ICES-003)

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

English translation of the notice above:

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

EC Declaration of Conformity

European Community Directives Requirement (CE)

Declaration of Conformity

Manufacturer's Name: 8e6 Technologies
Manufacturer's Address: 828 W. Taft Avenue
Orange, CA 92865

Application of Council Directive(s): Low Voltage • 2006/95/EC
EMC • 2004/108/EC

Standard(s): Safety • EN60950: 2006
EMC • EN55022: 2006
• EN55024: 1998 +A2:2003
• EN61000-3-2: 2000
• EN61000-3-3: 2001

Product Name(s): Internet Appliance

Product Model Number(s): MSA-004-005

Year in which conformity is declared: 2008

All hardware components supplied in this unit's shipping carton are certified by our vendors to be RoHS compliant.

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

Location: Orange, CA, USA

Signature:



Date: January 21, 2008

Full Name: Gregory P. Smith

Position: Director of Engineering Operations

INDEX

A

Activate and Register the ProxyBlocker 38

B

Boot Up 28

C

crossover cable 19, 28, 36

E

EMC 43, 44

F

FCC 43

H

HyperTerminal Setup 21

I

ICES-003 43

L

Login screen 24

Log in to ProxyBlocker Administrator Console 30, 37

LVD 43

M

MSA 20, 28, 42, 43

P

Physically Connect the ProxyBlocker to the Network 36

Power Supply Precautions 15

R

R3000 1

Rack Setup Precautions 6

reboot 31, 36

RoHS compliant 44

S

serial port cable 4, 19, 20

shut down 36

U

UL 43

W

wizard setup 19, 26

8e6 Corporate Headquarters (USA):
828 West Taft Avenue Orange, CA 92865-4232 • Tel: 714.282.6111 or 888.786.7999
Fax: 714.282.6116 (Sales/Technical Support) • 714.282.6117 (General Office)

Satellite Office:
8e6 Taiwan: 7 Fl., No. 1, Sec. 2, Ren-Ai Rd., Taipei 10055, Taiwan, R.O.C.
Tel: 886-2-2397-0300 • Fax: 886-2-2397-0306